Computers and Digital Evidence

813.1 PURPOSE AND SCOPE

This policy establishes procedures for the seizure and storage of computers, personal communications devices (PCDs), digital cameras, digital recorders and other electronic devices that are capable of storing digital information; and for the preservation and storage of seized digital evidence. All evidence seized and/or processed pursuant to this policy shall be done so in compliance with clearly established Fourth Amendment and search and seizure provisions.

This policy does not address the disposition of recordings by body worn cameras or those created in compliance with mandatory electronic recording requirements.

813.2 SEIZING COMPUTERS AND RELATED EVIDENCE

Computer equipment requires specialized training and handling to preserve its value as evidence. Officers should be aware of the potential to destroy information through careless or improper handling, and utilize the most knowledgeable available resources. When seizing a computer and accessories, the following steps should be taken:

(a) Photograph each item, front and back, specifically including cable connections to other items. Look for a phone line or cable to a modem for Internet access.

(b) Do not overlook the possibility of the presence of physical evidence on and around the hardware relevant to the particular investigation such as fingerprints, biological or trace evidence, and/or documents.To safeguard against the possibility of destroying physical evidence, where latex gloves when handling these items.

(c) If the computer is off, do not turn it on.

(d) If the computer is on, move the mouse or touch any key to awake the computer.

1. Photograph the screen, if possible, and note any programs or windows that appear to be open and running.

    (a) If it **appears** there is any program open and running, do not do anything with the computer and immediately contact any member of the Digital Evidence Cybercrime Unit (DECU) for assistance and instruction.

    (b) If it does **not appear** any program is running, disconnect the power cable from the back of the computer box or if a portable notebook style, disconnect and power cable from the case and remove the battery.

(e) Label each item with case number, evidence sheet number, and item number.

(f) Handle and transport the computer and storage media (e.g., tape, discs, memory cards, flash memory, external drives) with care so that potential evidence is not lost.

(g) Lodge all computer items in the Property Room. Do not store computers where normal room temperature and humidity is not maintained.

(h) At minimum, officers should document the following in related reports:

1. Where the computer was located and whether or not it was in operation.

2. Who was using it at the time.
3. Who claimed ownership.
4. If it can be determined, how it was being used.

(i) In most cases when a computer is involved in criminal acts and is in the possession of the suspect, the computer itself and all storage devices (hard drives, tape drives, and disk drives) should be seized along with all media. Accessories (printers, monitors, mouse, scanner, keyboard, cables, software and manuals) should not be seized unless as a precursor to forfeiture.

(j) Since most laptops have proprietary power cords, seize the power cord as well as the laptop being taken as evidence.

813.2.1 BUSINESS OR NETWORKED COMPUTERS

If the computer belongs to a business or is part of a network, it may not be feasible to seize the entire computer. Cases involving networks require specialized handling. Officers should contact a certified forensic computer examiner for instructions or a response to the scene.

It may be possible to perform an on-site inspection, or to image the hard drive only of the involved computer. This should only be done by someone specifically trained in processing computers for evidence.

813.2.2 FORENSIC EXAMINATION OF COMPUTERS

If an examination of the contents of the computer's hard drive, or floppy disks, compact discs, or any other storage media is required, forward the following items to a computer forensic examiner:

(a) Copy of report(s) involving the computer, including the Evidence/Property sheet.

(b) Copy of a consent to search form signed by the computer owner or the person in possession of the computer, or a copy of a search warrant authorizing the search of the computer hard drive for evidence relating to investigation.

(c) A listing of the items to search for (e.g., photographs, financial records, e-mail, documents) including any known relevant "keywords" such as victim's names, addresses, credit card numbers or other information related to the investigation.

(d) A forensic copy of a drive or disk will be made using a forensic computer and a forensic software program by someone trained in the examination of computer storage devices for evidence.

813.3 SEIZING DIGITAL STORAGE MEDIA

Digital storage media (e.g., hard discs, floppy discs, CDs, DVDs, tapes, memory cards, flash memory devices) should be seized and stored in a manner that will protect them from damage.

(a) Do not review, access or open digital files prior to submission.

(b) Many kinds of storage media can be erased or damaged by magnetic fields. Keep all media away from magnetic devices, electric motors, radio transmitters or other sources of magnetic fields.

(c) Do not leave storage media where they would be subject to excessive heat such as in a parked vehicle on a hot day.

(d) Use plastic cases designed to protect the media, or other protective packaging, to prevent damage. Then place the item into the appropriate size paper evidence envelope for submission into property.

813.4 SEIZING PERSONAL COMMUNICATION DEVICES

Personal communication devices (PCD) such as cell phones or other hand-held devices connected to any communication network must be handled with care to preserve evidence that may be on the device including messages, stored data and/or images.

(a) Officers should not attempt to access, review or search the contents of such devices prior to examination by a forensic expert. Unsent messages can be lost, data can be inadvertently deleted and incoming messages can override stored messages.

(b) If unable to turn the device off, either place the item into "airplane" mode or remove the battery.

(c) When seizing the devices, also seize the charging units and keep them plugged in to the chargers until they can be examined. If the batteries go dead all the data may be lost.

(d) If possible, obtain any pass codes or pattern locks.

813.5 DIGITAL EVIDENCE RECORDED BY OFFICERS

Officers handling and submitting recorded and digitally stored evidence from digital cameras and audio or video recorders will comply with these procedures to ensure the integrity and admissibility of such evidence.

When confronted with a case where they are unsure how to proceed with the collection of any type of digital evidence, officers should contact a member of the Digital Evidence Cybercrime Unit (DECU) for assistance.

813.5.1 COLLECTION OF DIGITAL EVIDENCE

Photographs of evidence taken by members of VPD shall be done with either a Department issued digital camera or their Department issued cell phone. Officers should not use their personal devices to take photographs since the devices could be subject to seizure at a later time.

Photographs of evidence taken with digital cameras should be uploaded to the RMS. Once uploaded, they can be deleted from the camera or phone used to take the photos.

813.5.2 ADULT NUDITY OR PORNOGRAPHY

If evidence photographs involve any type of adult nudity or pornography, the photographs should generally not be uploaded into the RMS but instead placed on a digital media device and submitted into evidence. This will prevent others from viewing the photos.If there is a need for a Department member to see the photos, they will have to contact evidence staff to arrange the transfer of the evidence.

a.Members should never have any type of images depicting adult nudity or pornography of any kind sent to them via email, nor should they ever send these types of images over email themselves.

813.5.3 CHILD PORNOGRAPHY

Child pornography, or photos of child pornography taken in the field by a Department member should not be uploaded into the RMS.Instead, photographs will be downloaded from the camera to removable storage media (e.g., SD card, flash drive, CD Rom) and placed into evidence.The outside of the evidence envelope should have a marking indicating that there is child pornography on the media.

a.Members should never have any type of images depicting child pornography of any kind sent to them via email, nor should they ever send these types of images over email themselves.

813.5.4 CLOUD BASED STORAGE

Officers confronted with a case where criminal evidence is found in an email or in a cloud-based storage site (e.g., Microsoft One Drive, Dropbox, Google Drive, etc.) have the following options:

a.Seize the computer the email or cloud storage is being accessed on and place into evidence following the evidence seizure criteria outlined in this policy.

b.Take photographs of the photos that are present on the screen, then later download onto a media storage device or upload into the RMS as appropriate.

c.Obtain all relevant information regarding the email or cloud storage account the child pornography is located on and, if appropriate, obtain a signed consent for its examination. Relevant information includes:

1.Account type (e.g., email, cloud storage, etc.),

2.Account name,

3.Account owner,

4.Logins, and;

5.Passwords.

Officers should take steps to preserve the account from tampering/destruction by sending a preservation letter to the appropriate Electronic Service Provider. If members are unsure how to complete this task, they should consult a member of the Digital Evidence Cybercrime Unit (DECU) for assistance.

813.6 INTERNET CRIMES AGAINST CHILDREN (ICAC) INVESTIGATIONS

Only sworn, on-duty ICAC trained personnel shall conduct ICAC investigations in an undercover capacity. Private citizens shall not be asked to seek out investigative targets nor shall they be authorized to act as police agents in any online undercover capacity.

Media releases relating to prosecutions, crime alerts, or other matters concerning online undercover (ICAC) operations shall not include information regarding confidential investigative techniques, shall not reveal the undercover operative information and should be coordinated (when applicable) with other Task Force participants (local, state or federal agencies) that may be involved in the investigation and shall be consistent with VPD media relations protocols.